Exhibit A

REESE RICHMAN LLP
Michael R. Reese (California State Bar No. 206773)
mreese@reeserichman.com
Kim E. Richman
krichman@reeserichman.com
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643 -0500
Facsimile: (212) 253-4272

Attorneys for Plaintiff and the Proposed Class

[Additional counsel on signature page]

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SAN FRANCISCO

MARK CARANDANG, on Behalf of Himself and All Others Similarly Situated,

Plaintiff,

v.

GOOGLE INC.,

Defendant.

Case No. CGC-12-518415

CLASS ACTION COMPLAINT

COMPLAINT FOR:

VIOLATION OF CALIFORNIA PENAL CODE § 502, VIOLATION OF ARTICLE I, SECTION 1 OF THE CALIFORNIA CONSTITUTION, VIOLATION OF CALIFORNIA PENAL CODE § 631 *ET SEQ.*, and COMMON LAW INVASION OF PRIVACY

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Plaintiff Mark Carandang ("Plaintiff") alleges the following, upon personal knowledge with respect to himself, and on information and belief derived from, among other things, investigation of counsel and review of public documents, as to all other matters:

NATURE OF THE ACTION

1. This is an action on behalf of a class of millions of California Internet users (the "Class," as defined herein) whose web browser privacy settings were bypassed by Google Inc. ("Google" or "Defendant").

2. For users of Apple Inc.'s Safari web browser ("Safari"), Google bypassed their settings when the users visited one or more websites displaying certain invasive advertisements served by Google. Google also bypassed the privacy settings of other browsers, such as Internet Explorer.

3. Within such advertisements, Google used surreptitious and invasive code – *i.e.*, computer programming language – to circumvent a Safari user's privacy settings without the user's knowledge and against the user's express will.

4. This circumvention enables Google – a company that has publicly promised to "Do No Evil" – to collect and store sensitive, private, and personally identifiable information ("PII") illegitimately.

5. Google's code circumvents a Safari (and other browser) user's privacy settings regardless of whether the user clicks on an ad and regardless of whether the user is logged in to Google.

6. These actions violate California Penal Code Section 502; Article I, Section 1 of the California Constitution; and California Penal Code Section 631 *et seq.*; and these actions constitute invasion of privacy and intentional misrepresentation under the common law of California.

JURISDICTION AND VENUE

7. This Court has jurisdiction over these proceedings because Google is headquartered in the State of California, transacts business within this State, has committed wrongful acts within the State, and has committed wrongful acts that have caused injuries to persons within the State.

8. Venue lies in this Court because Google conducts substantial business in this county; many of the Internet users affected by Defendant's wrongful conduct, including Plaintiff, reside in this county; and many of the potential witnesses reside and work in this county.

THE PARTIES

9. Plaintiff Mark Carandang resides in San Francisco. Mr. Carandang is a Safari user who used his iPhone to visited websites, such as YouTube.com, that displayed advertisements served by Google and contained the invasive code at issue. Safari was Mr. Carandang's primary iPhone browser, and his privacy settings prohibited third party tracking. Mr. Carandang also browses using Internet Explorer on his computer. Mr. Carandang is also a Google account holder. Google used the invasive code contained in said advertisements to circumvent Mr. Carandang's Safari privacy settings without his knowledge and against his express will. Google not only circumvented Mr. Carandang's Safari privacy settings, but it did so for the purpose of tracking and collecting Mr. Carandang's browsing history and linking it to PII. Mr. Carandang was not aware of, and would not have consented to, his Safari privacy settings being circumvented by Google in this manner. Mr. Carandang was not aware that his personal information or web browsing history was being collected by Google in this manner, and, indeed, had explicitly prohibited such actions.

10. Defendant Google Inc. is a Delaware Corporation that maintains its headquarters in Santa Clara County, California. Google conducts business throughout California, the nation, and internationally.

STATEMENT OF FACTS:

Google

11. Google provides, among many other services, an Internet search engine that enables users of the World Wide Web to locate websites. According to web information company Alexa, Google's search engine is the most highly trafficked website in the United States and the world. *See* http://www.alexa.com/siteinfo/google.com#.

12. Google also provides a variety of advertising services for the world's buyers, creators, and sellers of digital advertising. In December 2011, Google delivered Internet ads that were viewed at least once by 93% of United States web users, according to *The Wall Street Journal*, citing a study by comScore Media Metrix.[1]

13. Google+ is a social networking service that enables users to create profiles and share personal information. Google encourages prospective Google+ users to "[s]hare your thoughts, links and photos with the right circles." *See* http://www.google.com/+/learnmore/.

14. The Google+ "Privacy Policy" states that:

[1] Julia Angwin & Jennifer Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, Wall St. J., Feb. 17, 2012, *available at* http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

> We will record information about your activity – such as posts you comment on and the other users with whom you interact – in order to provide you and other users with a better experience on Google services.
>
> We may also collect information about you from other users, such as when someone puts you in one of their circles or tags you in a photo. Some users may choose to display information about you publicly, such as by displaying your public profile name and photo on their Google Profile in a list of people they've added to their circles.

See http://www.google.com/intl/en/+/policy/.

15. Google requires that Google+ registrants provide their actual names, rather than merely create a "screen name" or "user name" as is commonplace with other, non-social networking website registrations.

16. Accordingly, Google has access to, observes, and records extensive intimate, personal information about Google+ users.

17. Recently, Google has been facing questions related to privacy. Last month, Google said it would revise its privacy policy to combine nearly all the information it possesses about its users, a move that prompted an international outcry. European Union ("EU") privacy officials, for example, asked Google to "pause" its changes until it can ensure the privacy of EU citizens. Google said it briefed European officials in the weeks before its announcement and plans to implement the new privacy policy March 1.

Google Circumvents the Privacy Settings of Users of the Safari Web Browser and Other Browsers

18. Unbeknownst to millions of Californians using Apple's Safari web browser on their mobile devices and computers, Google has been bypassing Safari's privacy settings, enabling itself to track the web browsing habits of people who intended for that kind of monitoring to be blocked. Google – despite its promise to "Do No Evil" – uses invasive code that tricks Safari's web browsing software into letting Google monitor users as they browse the Internet, thereby

collecting private and, in some cases, sensitive information about them – without their knowledge and against their express will. Safari, the most widely used browser on mobile devises, is designed to block such tracking by default.

19. Once the code is activated for a single advertisement, Google can track a user across the vast majority of websites on the World Wide Web.

20. Stanford researcher Jonathan Mayer first identified the invasive Google code. Subsequently, Ashkan Soltani, technology adviser for *The Wall Street Journal*, independently confirmed Mr. Mayer's findings. Mr. Soltani surveyed the top 100 most popular websites as ranked by Quantcast in February 2012. He found that Google placed the invasive code within ads displayed on major web sites, including movie site Fandango.com, dating site Match.com, AOL.com, TMZ.com, and UrbanDictionary.com, among others.

21. On February 17, 2012, *The Wall Street Journal* published an article describing these findings in detail. *See* Julia Angwin & Jennifer Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, Wall St. J., Feb. 17, 2012, *available at* http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html.

\\

\\

\\

\\

\\

\\

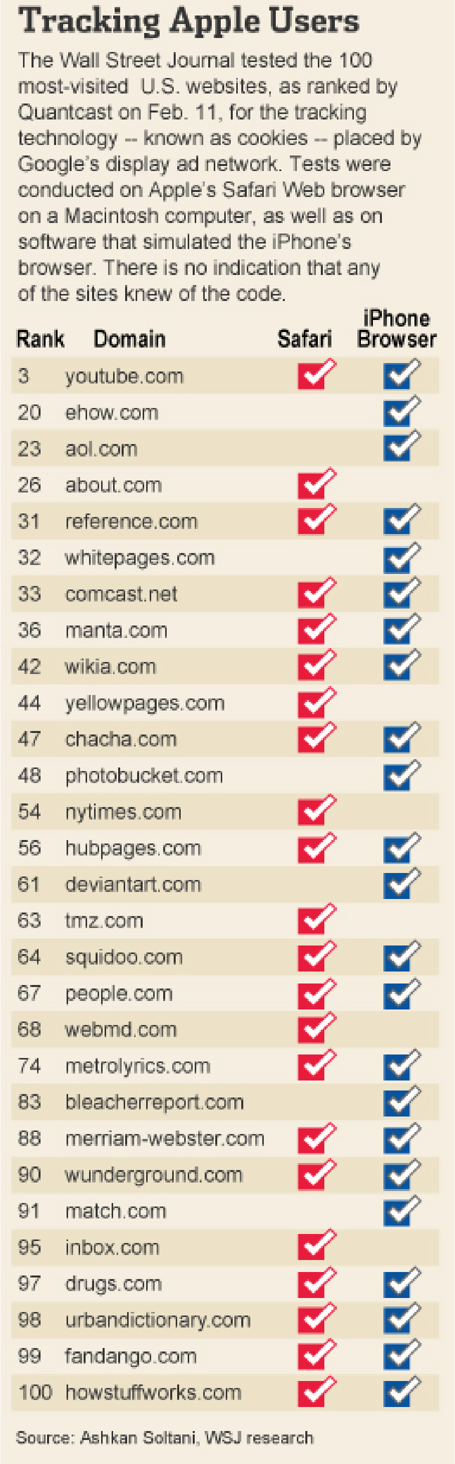
\\

\\

\\

\\

22. Regarding sites that displayed advertisements containing the invasive code, Mr. Soltani's findings are summarized in the following graphic that was published in *The Wall Street Journal* article:



Tracking Apple Users

The Wall Street Journal tested the 100 most-visited U.S. websites, as ranked by Quantcast on Feb. 11, for the tracking technology -- known as cookies -- placed by Google's display ad network. Tests were conducted on Apple's Safari Web browser on a Macintosh computer, as well as on software that simulated the iPhone's browser. There is no indication that any of the sites knew of the code.

Rank	Domain	Safari	iPhone Browser
3	youtube.com	✓	✓
20	ehow.com		✓
23	aol.com		✓
26	about.com	✓	
31	reference.com	✓	✓
32	whitepages.com		✓
33	comcast.net	✓	✓
36	manta.com	✓	✓
42	wikia.com	✓	✓
44	yellowpages.com	✓	
47	chacha.com	✓	✓
48	photobucket.com		✓
54	nytimes.com	✓	
56	hubpages.com	✓	✓
61	deviantart.com		✓
63	tmz.com	✓	
64	squidoo.com	✓	✓
67	people.com	✓	✓
68	webmd.com	✓	
74	metrolyrics.com	✓	✓
83	bleacherreport.com		✓
88	merriam-webster.com	✓	✓
90	wunderground.com	✓	✓
91	match.com		✓
95	inbox.com	✓	
97	drugs.com	✓	✓
98	urbandictionary.com	✓	✓
99	fandango.com	✓	✓
100	howstuffworks.com	✓	✓

Source: Ashkan Soltani, WSJ research

Id.

23. Google's invasive tracking of Safari users stems from Google's use of a "+1" button in conjunction with Google's social network, Google+. Google+ was hastily launched on June 28, 2011, without proper privacy safeguards and systems, to compete with and halt the loss of Google users to the Facebook social network. Similar to Facebook's "Like" button, the "+1" button gives people an easy way to indicate that they like various things online.

24. In 2011, Google added a feature to connect the "+1" feature to online advertisements. Using its DoubleClick advertising technology, Google enabled Internet users to click on a "+1" button in an advertisement, which would then link the advertisement to the Google+ profile of each user who clicked on the button.

25. However, Google faced a problem. Safari blocks most tracking by default. As a result, Google could not use the most common tracking technique – installation of a file known as a "cookie" – to check whether Safari users were logged in to Google.

26. To get around Safari's default blocking, Google exploited a loophole in Safari's privacy settings. While Safari does block most tracking, it makes an exception for websites with which a person interacts in some way – for instance, by filling out a form. In order to exploit this exception, Google added coding to some of the ads it served that tricked Safari into performing as if a user were submitting an invisible form to Google. As a result of being deceived in this manner, Safari allowed Google to install a cookie on the user's mobile device or computer.

27. The cookie that Google installed on the mobile device or computer was temporary; it expired in 12 to 24 hours. This original cookie, however, resulted in many cases in extensive tracking of Safari users. This is because of a technical quirk in Safari that allows companies to easily add more cookies to a user's mobile device or computer once the company has installed at least one cookie.

28. Google used these tracking cookies to collect extensive information about the web browsing habits of Internet users – even when the users had never clicked on a "+1" button and ***even though the users had requested that Google refrain from tracking them***. If these Internet users sought advice about hemorrhoids, sexually transmitted diseases, abortion, drug rehabilitation, dementia, etc., Google could be reasonably certain to have observed and recorded that web browsing – ***in spite of the fact that the Safari users had specifically instructed that third parties like Google should not be allowed to track them, even anonymously***.

29. In the case of Google+ account holders that were logged in to Google+ and browsing via Safari when they viewed the ad containing invasive code, the cookie that Google installed on the user's mobile device or computer contained encoded information about that user's Google+ account. Google thereby linked:

(a) the personal information, thoughts, photographs, etc., that Google+ account holders provided on their Google+ accounts, with

(b) Safari browsing histories that Google obtained against the Google+ users' express wishes.

To put it simply, in the case of Google+ users, not only did Google obtain an anonymous browsing history that it had no permission to obtain, it de-anonymized and personalized that illegitimately-gained browsing history. For an illustration of how this process worked, refer to Exhibit 1 hereto.

The Value to Google of Users' Personal Information

30. The personal information collected by Google is an asset of the sort that is priced, bought, and sold in discrete units for marketing and other purposes. "Websites and stores can . . . easily buy and sell information on valued visitors with the intention of merging behavioral with demographic and geographic data in

ways that will create social categories that advertisers covet and target with ads tailored to them or people like them." Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, & Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214. The more information that is known about a consumer, the more a company will pay to deliver a precisely targeted advertisement to him or her. *See* Federal Trade Commission (FTC), Protecting Consumer Privacy in an Era of Rapid Change, Preliminary Staff Report (Dec. 2010) ("FTC Report"), at 24.

31. Personal data is viewed as currency. "In many instances, consumers pay for free content and services by disclosing their personal information," according to former FTC commissioner Pamela Jones Harbour. FTC Roundtable Series 1 on: Exploring Privacy (Matter No. P095416) (Dec. 7, 2009), at 148, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/ PrivacyRoundtable_Dec 2009_Transcript.pdf. In *Property, Privacy, and Personal Data*, Professor Paul M. Schwartz wrote:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

32. On February 28, 2011, *The Wall Street Journal* highlighted a company called "Allow Ltd.," which is one of nearly a dozen companies that offers to sell people's personal information on their behalf and which gives its users 70% of such sales. *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, Wall St. J., Feb. 28, 2011, *available at* http://online.wsj.com/article/

SB10001424052748703529004576160764037920274.html. For example, one Allow Ltd. user received a payment of $8.95 for letting Allow tell a credit card company the user was shopping for a new credit card. *Id.*

33. On February 15, 2012, *The Financial Times* acknowledged the value of personal information in the Internet age in the context of Facebook, Inc.'s upcoming initial public offering: "Two weeks ago Facebook announced an initial public offering that could value the company at up to $100bn. Facebook is worth so much because of the data it holds on its 845m users."[2]

34. As noted in the *Wall Street Journal*, "[t]rade in personal data has emerged as a driver of the digital economy. Many tech companies offer products for free and get income from online ads that are customized using data about customers. These companies compete for ads, in part, based on the quality of the information they possess about users." Angwin & Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*.

35. Moreover, Google itself acknowledges the value of web browsing histories – for example, by purchasing such histories directly from web users. Google's "Screenwise" panel is a program whereby a few thousand Google users are allowing Google to track their web browsing histories in return for up to $25 in gift cards. *See* http://www.google.com/landing/screenwisepanel/.

Google Misrepresented the Effect of Safari's Privacy Settings on Google Tracking

36. According to the February 17, 2012 *Wall Street Journal* article:

> In Google's case, the findings [of Jonathan Mayer and Ashkan Soltani] appeared to contradict some of Google's own instructions to Safari users on

[2] Richard Falkenrath, *Google Must Remember Our Right to be Forgotten*, Fin, Times, *available at* http://www.ft.com/intl/cms/s/0/476b9a08-572a-11e1-869b-00144feabdc0.html#axzz1mgPiI5Ux.

> how to avoid tracking. Until recently, one Google site told Safari users they could rely on Safari's privacy settings to prevent tracking by Google. Google removed that language from the site Tuesday night.

See Angwin & Valentino-Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*; *see also* Exhibit 2 (screenshot of the historical Google webpage providing instructions to Safari users).

37. Accordingly, Google represented to Safari users – and World Wide Web users in general – that Safari's privacy settings were sufficient to prevent Google from tracking them, even though Google had intentionally implemented invasive code designed specifically to circumvent Safari's privacy settings in order to track Safari users.

38. On Friday, February 17, three congressmen, Edward J. Markey (D., Mass.), Joe Barton (R., Texas), and Cliff Stearns (R., Fla.), called on the FTC to investigate Google in relation to the violations of law described herein, wanting to know whether Google's behavior constitutes a violation of a privacy settlement Google and the FTC signed in 2011. Among other things, the FTC settlement barred Google from misrepresenting its privacy policy to users. Breaches of the settlement could bring fines of as much as $16,000.00 per violation per day. *See* Jennifer Valentino-Devries, *Lawmakers Target Google's Tracking*, Wall St. J., Feb. 18, 2012, *available at* http://online.wsj.com/article/ SB10001424052970204059804577229681587016516.html.

39. At least two consumer groups have also requested that the FTC investigate Google's behavior. *Id.*

CLASS ACTION ALLEGATIONS

40. Pursuant to section 382 of the California Code of Civil Procedure, Plaintiff brings this action on behalf of himself and the following class of Internet users (collectively, the "Class"):

> All Internet users who, while residing in California, visited a website that contained a mechanism – such as an advertisement served by Google containing invasive code – that circumvented the users' web browser privacy settings and placed a cookie on the users' mobile device and/or computer, from the date that such circumvention began to the date of filing of this complaint (the "Class Period").

41. This action is properly maintainable as a class action.

42. The Class is so numerous that joinder of all members is impracticable. There are millions of Internet users in the State of California whose browser privacy settings have been circumvented by Google.

43. There are questions of law and fact that are common to the Class including, *inter alia*, the following:

(a) whether Google hacked the browser privacy settings of Plaintiff and the Class, in violation of California Penal Code § 502;

(b) whether Google engaged in conduct that invaded the privacy interests of Plaintiff and the Class;

(c) whether Plaintiff and the Class had a reasonable expectation of privacy as to the interests invaded;

(d) whether the invasion of privacy was serious;

(e) whether this invasion of privacy caused Plaintiff and the Class to suffer injury, damage, loss, or harm; and

(f) whether Google violated California Penal Code § 631 *et seq.*

44. Plaintiff will fairly and adequately represent the Class. Plaintiff is committed to prosecuting this action and has retained competent counsel experienced in litigation of this nature. Plaintiff's claims are typical of the claims of other members of the Class, and Plaintiff has the same interests as the other members of the Class.

45. Plaintiff anticipates no difficulty in the management of this litigation.

46. Defendant has acted in a manner that affects Plaintiff and all Class members alike, thereby making appropriate injunctive, declaratory, and other relief appropriate with respect to the Class as a whole.

47. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, establish incompatible standards of conduct for defendants or adjudications with respect to individual members of the Class, and could be dispositive of the interests of other members or substantially impair or impede their ability to protect their interests.

FIRST CAUSE OF ACTION

Violation of
California Comprehensive Computer Data Access and Fraud Act (CCDAF)
California Penal Code § 502

48. Plaintiff incorporates each and every allegation of the Class Action Complaint above as if fully set forth herein.

49. In violation of California Penal Code § 502(c)(1), Google knowingly accessed and without permission altered, damaged, and/or otherwise used data, computers, computer systems, and/or computer networks to:

(A) execute a scheme or artifice to defraud or deceive, and/or

(B) wrongfully control or obtain money, property, or data,

Specifically, Google intentionally and without permission used invasive code for the purpose of circumventing Plaintiff's and the Class members' web browser privacy settings, rendering them useless (effectively, altering them). In spite of the fact that these privacy settings denied Google permission to track Plaintiff and the Class's web browsing, Google placed cookies on said computers and/or mobile devices that Google used to wrongfully obtain data (e.g., browsing histories).

Google circumvented Plaintiff's and the Class members' web browser privacy settings and placed tracking cookies on their computers and/or mobile devices as part of the execution of a scheme to defraud and/or deceive Plaintiff and the Class, who believed their Safari privacy settings protected them from being tracked in this manner.

50. In violation of California Penal Code § 502(c)(2), Google knowingly accessed and without permission took, copied, and/or made use of data from a computer, computer system, and/or computer network. Specifically, Google intentionally and without permission circumvented Plaintiff's and the Class members' web browser privacy settings in order to acquire data from Plaintiff's and the Class members' computers and/or mobile devices.

51. In violation of California Penal Code § 502(c)(3), Google knowingly and without permission used "computer services" as that term is defined in California Penal Code § 502(b)(4), including storage functions and web history tracking. Specifically, Google intentionally and without permission stored cookies on Plaintiff's and the Class members' computers and/or mobile devices and used those cookies in conjunction with Plaintiff's and the Class members' computers and/or mobile devices to track Plaintiff and the Class members.

52. In violation of California Penal Code § 502(c)(4), Google knowingly and without permission added, altered, and/or damaged data, computer software, and/or computer programs that resided and/or existed internal and/or external to a computer, computer system, and/or computer network. Specifically, Google intentionally and without permission circumvented Plaintiff's and the Class members' web browser privacy settings, rendering them useless (effectively, altering them). Furthermore, Google intentionally and without permission added cookies to Plaintiff's and the Class members' computers and/or mobile devices.

53. In violation of California Penal Code § 502(c)(5), Google knowingly and without permission disrupted and/or caused the disruption of "computer

services" (as that term is defined in California Penal Code § 502(b)(4)) to an authorized user of a computer, computer system, and/or computer network. Specifically, Google intentionally and without permission disrupted the functionality and effectiveness of Plaintiff's and the Class members' web browser privacy settings, thereby disrupting Plaintiff's and the Class members' desired use of their web browsers.

54. In violation of California Penal Code § 502(c)(7), Google knowingly and without permission accessed computers, computer systems, and/or computer networks. Google intentionally and without permission circumvented Plaintiff's and the Class members' web browser privacy settings and placed cookies on Plaintiff's and the Class members' computers and/or mobile devices. Google used these cookies to illegitimately obtain Plaintiff's and the Class members' web browsing histories.

55. In violation of California Penal Code § 502(c)(8), Google knowingly introduced "computer contaminants" – as defined in California Penal Code § 502(b)(10) – into computers, computer systems, and/or computer networks. Specifically, Google intentionally introduced invasive code into Plaintiff's and the Class members' computers and/or mobile devices that "usurp[ed] the normal operation" of said computers and/or mobile devices by circumventing the users' web browser privacy settings and placing cookies on said computers and/or mobile devices.

56. As a direct and proximate result of Google's violation of California Penal Code § 502, Google caused loss to Plaintiff and the Class in an amount to be proven at trial. Plaintiff and the Class are entitled to recovery of attorneys' fees pursuant to § 502(e).

57. Plaintiff and the Class are entitled to punitive or exemplary damages under California Penal Code § 502(e)(4) because Google willfully violated § 502(c) and is guilty of "fraud" as defined by California Civil Code § 3294(c)(3).

Under § 3294(c)(3), "fraud" means an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury. Google intentionally concealed from Plaintiff and the Class the fact that Google debilitated the privacy safeguards established by Plaintiff and the Class's web browser privacy settings. As a result of concealing this fact, Google intended to and did deprive Plaintiff and the Class of their legal right to privacy. Furthermore, Google intended to profit and did profit from this invasion of privacy by illegitimately obtaining Plaintiff and the Class's web browsing histories and selling them or otherwise using them in connection with Google's advertising services. Google thereby deprived Plaintiff and the Class of valuable property.

58. Plaintiff and the Class have also suffered irreparable injury as a result of Google's unlawful conduct, including the collection and sharing of their personal information. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiff and the Class have no adequate remedy at law, entitling them to injunctive relief.

SECOND CAUSE OF ACTION

Violation of Article I, Section 1 of the California Constitution

59. Plaintiff incorporates each and every allegation of the Class Action Complaint above as if fully set forth herein.

60. Article I, Section 1 of the California Constitution states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

61. Plaintiff and Class members had a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their computers and/or mobile devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy settings, which are individually customizable in accordance with the will of each browser user.

62. Plaintiff and the Class members had a legally protected privacy interest in the confidential and sensitive information (including browsing histories) that Google obtained by exploiting and circumventing Plaintiff's and the Class members' web browser privacy settings.

63. Plaintiff and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their computers and mobile devices free of interference, including decisions related to web browser privacy settings.

64. Plaintiff and the Class members reasonably expected that their confidential and sensitive information and intimate personal decisions would be kept private, especially for users who affirmatively requested not to be tracked.

65. Google committed a serious invasion of Plaintiff's and the Class members' privacy interests by circumventing their web browser privacy settings. Unbeknownst to Plaintiff and Class members, Google made a private decision on behalf of Plaintiff and the Class that Google was not authorized to make.

66. Google committed a serious invasion of Plaintiff's and Class members' privacy interests by, as a result of circumventing Plaintiff's and Class members' web browser privacy settings, placing cookies on Plaintiff's and the Class members' computers and/or mobile devices, enabling Google to track Plaintiff's and Class members' browsing histories without their knowledge and against their express will. The seriousness of the invasion was compounded by the fact that Google was able to link those illegitimately-obtained browsing histories with private, sensitive, or personal information contained in Google+ accounts.

67. By the acts, transactions, and courses of conduct alleged herein, Defendant violated Plaintiff's and the Class members' inalienable right to privacy.

THIRD CAUSE OF ACTION

California Invasion of Privacy Act

California Penal Code § 631 *et seq*.

68. Plaintiff incorporates each and every allegation of the Class Action Complaint above as if fully set forth herein.

69. In violation of California Penal Code § 631, the communications of Plaintiff and Class members with third-party websites were intentionally obtained by Google while in transit over wires, lines, cables, or instruments through the State of California and while they were being sent from or received at a place within California.

70. Google willfully, intentionally, and without the consent of Plaintiff and the Class members, or any party to the communications, and in an unauthorized manner using an unauthorized connection, obtained, read, attempted to read, and learned, and attempted to learn the contents of such electronic communications of Plaintiff and the Class members while they were in transit in or through California.

71. Google used and communicated such illegally obtained electronic communications of Plaintiff and the Class members.

72. As a direct and proximate result of the above-described conduct by Google, Plaintiff and all Class members have suffered, and, unless such conduct is enjoined, will continue to suffer, damages in an amount to be proven at trial.

73. Pursuant to California Penal Code § 637.2, Plaintiff and the Class members are entitled to recover three times their actual and/or statutory damages from Google, for such conduct.

74. Google's conduct is causing, and unless enjoined will continue to cause, Plaintiff and the Class great and irreparable injury that cannot be fully compensated for or measured in money. Plaintiff and the Class have no adequate remedy at law and, pursuant to California Penal Code § 637.2(b), are entitled to preliminary and permanent injunctions prohibiting further use and communication of their unlawfully obtained information.

FOURTH CAUSE OF ACTION

Common Law Invasion of Privacy

75. Plaintiff hereby incorporates each and every allegation in the Class Action Complaint above as if fully set forth herein.

76. Google intruded on Plaintiff's and the Class members' private affairs and seclusion by circumventing Plaintiff's and the Class members' web browser privacy settings and placing cookies on their mobile devices and/or computers – conduct that Google engaged in completely outside of Plaintiff's and the Class members' knowledge and against their express will. These cookies enabled Google to track Plaintiff's and the Class members' web browsing histories and link those browsing histories with personal information contained in Google+ accounts, as more fully detailed herein.

77. Plaintiff and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their computers and mobile devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy settings, which are individually customizable in accordance with the will of each web browser user.

78. Plaintiff and the Class members have a legally protected privacy interest in the confidential and sensitive information (including browsing histories)

that Google obtained by exploiting and circumventing Plaintiff's and the Class members' web browser privacy settings.

79. Plaintiff and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their computers and mobile devices free of interference, including decisions related to web browser privacy settings.

80. Plaintiff and the Class reasonably expected that their confidential and sensitive information and intimate personal decisions would be kept private, especially for users who affirmatively requested not to be tracked.

81. Google intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by surreptitiously using invasive code to circumvent Plaintiff's and the Class members' web browser privacy settings, rendering them effectively useless. Unbeknownst to Plaintiff and the Class members, Google made a private decision on behalf of Plaintiff and the Class members that Google was not authorized to make.

82. Moreover, Google intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by, as a result of hacking into and subverting Plaintiff's and the Class members' web browser privacy settings, placing cookies onto Plaintiff's and the Class members' mobile devices and/or computers that enabled Google to track Plaintiff's and the Class members' web browsing activities and link those activities with personal information contained in Google+ accounts.

83. As a consequence, Plaintiff and the Class members were personally injured and suffered emotional distress damages.

FIFTH CAUSE OF ACTION

Intentional Misrepresentation

84. Plaintiff incorporates each and every allegation in the Class Action Complaint above as if fully set forth herein.

85. During the Class Period, Google engaged in fraudulent, misrepresentative, false, and/or deceptive practices. Google represented to Plaintiff and the Class that Safari's privacy settings were effective at preventing Google from tracking Plaintiff's and the Class members' Safari browsing, knowing that Google was in fact circumventing Safari's privacy settings with the specific purpose of tracking Plaintiff's and the Class members' Safari browsing.

86. These aforementioned frauds, misrepresentations, deceptive, and/or false acts and omissions concerned material facts that were essential to Plaintiff's and the Class members' decisions to browse the web using Safari, as opposed to the variety of other available web browsers that provide protections against third party tracking (e.g., Mozilla Firefox or Internet Explorer).

87. Plaintiff and the Class members would have acted differently had they not been misled but, instead, had been informed that Safari's privacy settings were ineffective at preventing Google from tracking Safari browsing because, contrary to Google's representations to Plaintiff and the Class, Google circumvented said privacy settings. Plaintiff and the Class members would not have browsed using Safari had they known this to be the case.

88. By and through such fraud, deceit, misrepresentations, and/or omissions, Google intended to induce Plaintiff and the Class members to alter their positions to their detriment.

89. Plaintiff and the Class members justifiably and reasonably relied on Google's omissions and misrepresentations, and, as such, were damaged by Google.

90. As a direct and proximate result of Google's omissions and misrepresentations, Plaintiff and the Class members have suffered damages.

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and members of the Class seek relief against defendant as follows:

A. Declaring that this action is properly maintainable as a class action and certifying Plaintiff as the representative of the Class;

B. Declaring that Google's actions, as described herein, violate California Penal Code § 502;

C. Declaring that Google's actions, as described herein, violate Article I, Section 1 of the California Constitution;

D. Declaring that Google's actions, as described herein, violate California Penal Code § 631 *et seq.*;

E. Declaring that Google's actions, as described herein, constitute an invasion of privacy under the common law;

F. Declaring that Google intentionally misrepresented information to Plaintiff and the Class, causing them damages, as described herein;

G. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including, *inter alia*, an order prohibiting Google from engaging in the wrongful and unlawful acts described herein;

H. Disgorgement of all revenue earned from selling or otherwise trading on the private information obtained from Plaintiff and the Class via invasive advertisements served by Google that circumvented Plaintiff and the Class members' web browser privacy settings, as described herein;

I. Awarding Plaintiff and the Class members statutory damages pursuant to California Penal Code § 637.2;

J. Awarding Plaintiff and the Class punitive or exemplary damages pursuant to California Penal Code § 502(e)(4);

K. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees; and

L. Awarding such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff and the Class hereby demand trial of their claims by jury to the extent authorized by law.

DATED: February 21, 2012

REESE RICHMAN LLP

Michael Reese

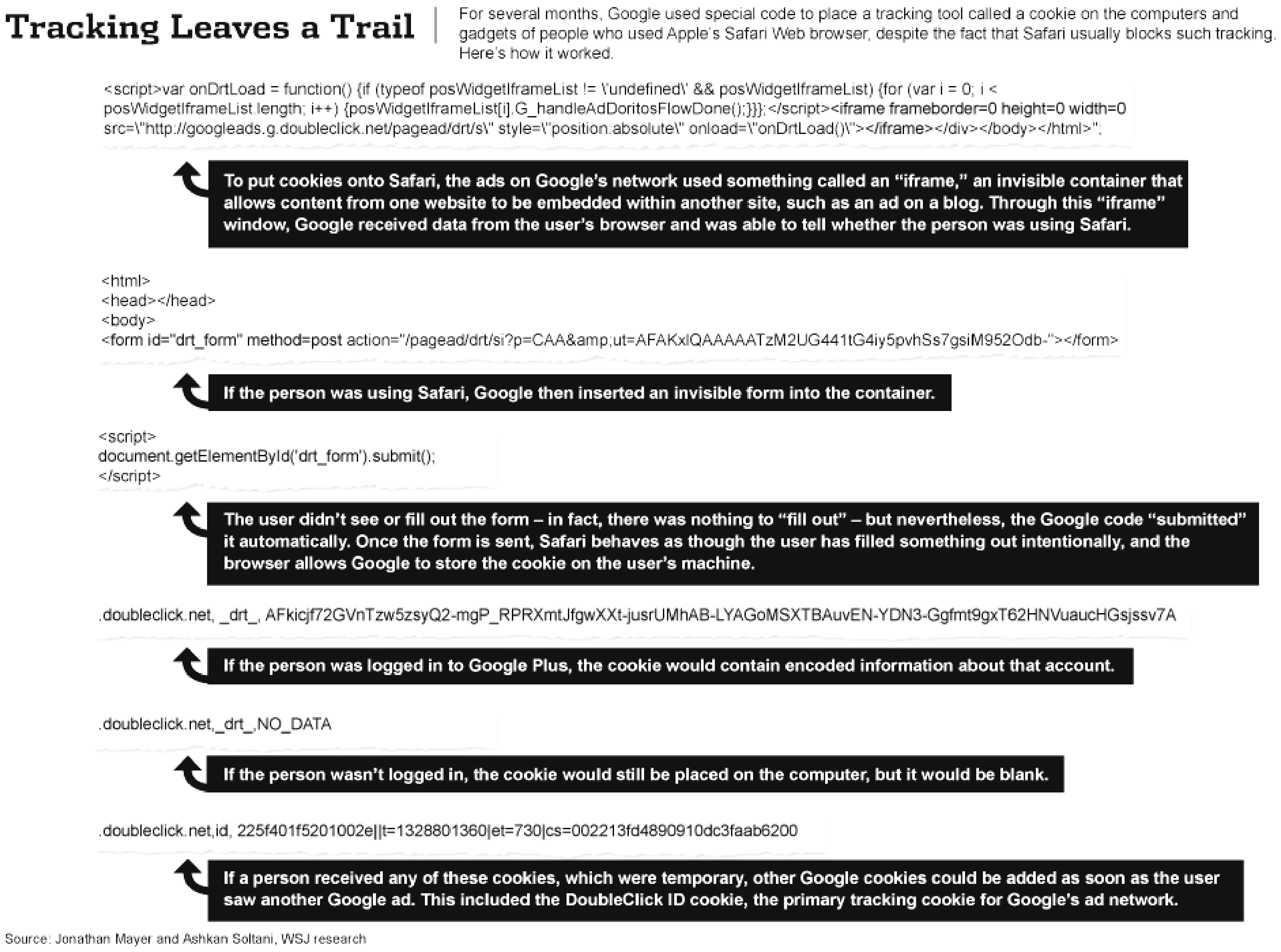
Michael R. Reese
mreese@reeserichman.com
Kim E. Richman
krichman@reeserichman.com
875 Avenue of the Americas, 18th Floor
New York, New York 10001
Telephone: (212) 643 -0500
Facsimile: (212) 253-4272

– and –

MILBERG LLP
Sanford P. Dumain
sdumain@milberg.com
Peter Seidman
pseidman@milberg.com
One Penn Plaza
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

Attorneys for Plaintiff and the Proposed Class

EXHIBIT 1



Tracking Leaves a Trail

For several months, Google used special code to place a tracking tool called a cookie on the computers and gadgets of people who used Apple's Safari Web browser, despite the fact that Safari usually blocks such tracking. Here's how it worked.

```
<script>var onDrtLoad = function() {if (typeof posWidgetIframeList != \'undefined\' && posWidgetIframeList) {for (var i = 0; i <
posWidgetIframeList.length; i++) {posWidgetIframeList[i].G_handleAdDoritosFlowDone();}}};</script><iframe frameborder=0 height=0 width=0
src=\"http://googleads.g.doubleclick.net/pagead/drt/s\" style=\"position.absolute\" onload=\"onDrtLoad()\"></iframe></div></body></html>";
```

To put cookies onto Safari, the ads on Google's network used something called an "iframe," an invisible container that allows content from one website to be embedded within another site, such as an ad on a blog. Through this "iframe" window, Google received data from the user's browser and was able to tell whether the person was using Safari.

```
<html>
<head></head>
<body>
<form id="drt_form" method=post action="/pagead/drt/si?p=CAA&amp;ut=AFAKxIQAAAAATzM2UG441tG4iy5pvhSs7gsiM952Odb-"></form>
```

If the person was using Safari, Google then inserted an invisible form into the container.

```
<script>
document.getElementById('drt_form').submit();
</script>
```

The user didn't see or fill out the form – in fact, there was nothing to "fill out" – but nevertheless, the Google code "submitted" it automatically. Once the form is sent, Safari behaves as though the user has filled something out intentionally, and the browser allows Google to store the cookie on the user's machine.

```
.doubleclick.net, _drt_, AFkicjf72GVnTzw5zsyQ2-mgP_RPRXmtJfgwXXt-jusrUMhAB-LYAGoMSXTBAuvEN-YDN3-Ggfmt9gxT62HNVuaucHGsjssv7A
```

If the person was logged in to Google Plus, the cookie would contain encoded information about that account.

```
.doubleclick.net,_drt_,NO_DATA
```

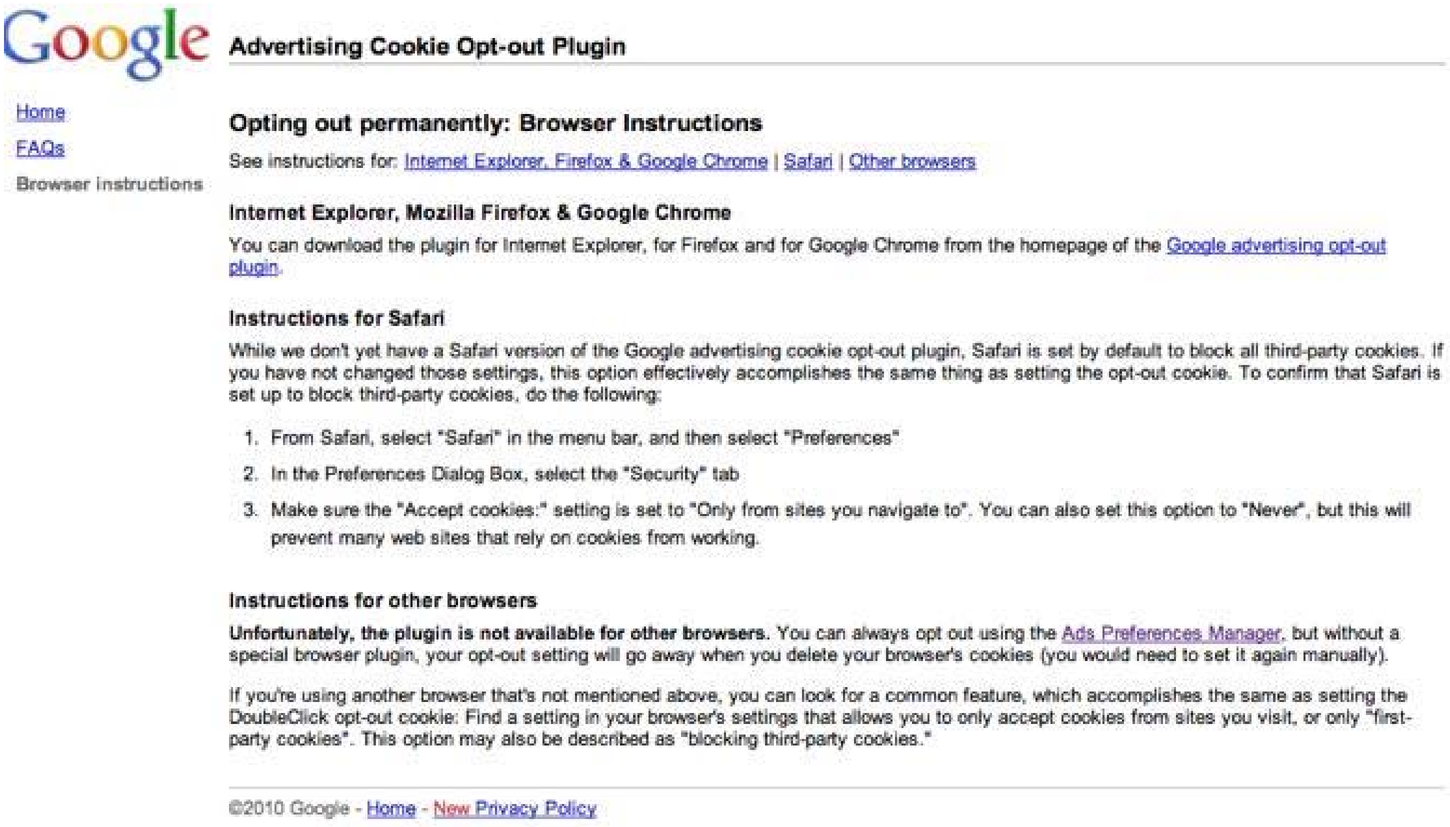
If the person wasn't logged in, the cookie would still be placed on the computer, but it would be blank.

```
.doubleclick.net,id, 225f401f5201002e||t=1328801360|et=730|cs=002213fd4890910dc3faab6200
```

If a person received any of these cookies, which were temporary, other Google cookies could be added as soon as the user saw another Google ad. This included the DoubleClick ID cookie, the primary tracking cookie for Google's ad network.

Source: Jonathan Mayer and Ashkan Soltani, WSJ research

EXHIBIT 2



Advertising Cookie Opt-out Plugin

Opting out permanently: Browser Instructions

See instructions for: Internet Explorer, Firefox & Google Chrome | Safari | Other browsers

Internet Explorer, Mozilla Firefox & Google Chrome

You can download the plugin for Internet Explorer, for Firefox and for Google Chrome from the homepage of the Google advertising opt-out plugin.

Instructions for Safari

While we don't yet have a Safari version of the Google advertising cookie opt-out plugin, Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the opt-out cookie. To confirm that Safari is set up to block third-party cookies, do the following:

1. From Safari, select "Safari" in the menu bar, and then select "Preferences"
2. In the Preferences Dialog Box, select the "Security" tab
3. Make sure the "Accept cookies:" setting is set to "Only from sites you navigate to". You can also set this option to "Never", but this will prevent many web sites that rely on cookies from working.

Instructions for other browsers

Unfortunately, the plugin is not available for other browsers. You can always opt out using the Ads Preferences Manager, but without a special browser plugin, your opt-out setting will go away when you delete your browser's cookies (you would need to set it again manually).

If you're using another browser that's not mentioned above, you can look for a common feature, which accomplishes the same as setting the DoubleClick opt-out cookie: Find a setting in your browser's settings that allows you to only accept cookies from sites you visit, or only "first-party cookies". This option may also be described as "blocking third-party cookies."